ABSTRACT OF THE DISCLOSURE

INCREMENTAL COMPLIANCE ENVIRONMENT, AN ENTERPRISE-WIDE SYSTEM FOR DETECTING FRAUD

A dynamically determined data-driven model for detecting fraudulent behavior is provided where statistically significant data elements are not known a priori. An initial model is developed using historical data, such as demographic, psychographic, transactional, and environmental data, using data-driven discovery techniques, such as data mining, and may be validated using additional statistical techniques. The noise within the data models determine appropriate initial control points needed for the initial model. These initial control points define an "electronic fence," wherein data points within the fence represent acceptable behavior and data points outside the fence represent unacceptable behavior. Updated data is received. A fraud detection mechanism validates the updated data using data mining and statistical methods. The data model, or "electronic fence," is refined based on the newly acquired data. The process of refining and updating the data models will be iterated until a set of limits is achieved. When the data models reach a steady state, the models will be treated as static models.